arXiv:1004.1127v2 [quant-ph] 7 May 2010

Quantum Generalized Reed-Solomon codes concatenated with random rate one inner stabilizer codes asymptotically attain the Quantum Gilbert-Varshamov bound

Yingkai Ouyang,
Department of Combinatorics and Optimization
University of Waterloo, Institute of Quantum Computing,
200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada
(y3ouyang@math.uwaterloo.ca)

May 10, 2010

Abstract

A good quantum code corrects for a linear number of errors. It has been shown that random codes attains the QGVB with a relative distance $H_{q^2}^{-1}((1-R)/2)$ where the code is q-ary and R is the rate of the code (number of encoded systems / block length). However, random codes have little structure. In this paper, we study a family of concatenated q-ary stabilizer codes. Each of the inner codes is a random rate 1 q-ary stabilizer code of block length n. The outer code is a quantum MDS code with block length q^n and alphabet size q^n, an arbitrary rate $R \leq 1$, and distance $N(1-R)/2+1$ that meets the Quantum Singleton bound. Fixing the outer code rate and letting n grow, the concatenated stabilizer code has a distance that almost surely attains the QGVB. This partially generalizes Thommesen's result, where he showed that the distance of a concatenated code with a Reed-Solomon outer code and random inner linear codes of arbitrary rate attains the Gilbert-Varshamov bound almost surely.

1 Introduction

A family of q-ary quantum codes of increasing block length is defined to be **good** if the ratio of its distance to its block length approaches a non-zero constant. Designing good quantum codes is highly nontrivial, just as it is in the classical case. The quantum Gilbert-Varshamov bound (QGVB) is a lower bound on an achievable relative distance of a quantum code of a fixed rate. Explicit constructions of good quantum codes for $q \leq 7$ have been studied [1, 2, 3], but they all fail to satisfy the QGVB. The QGVB bound is attainable for the family of all random quantum codes [4], the family of random stabilizer codes [5], and the family of random nondegenerate stabilizer codes [6], and the family of random degenerate stabilizer codes [6]. We show that concatenated quantum codes, with a quantum outer code having a known structure and being efficiently decodable, and randomly chosen independent inner quantum codes also attains the QGVB. Thus our family of random quantum codes has more structure than previously studied examples.

In this paper, we generalize a special case of Thommesen's result [7] to the quantum case. He showed that a code from the family of binary concatenated codes made with a

Reed-Solomon outer code and random rate one linear inner codes almost surely attains the Gilbert-Varshamov bound. A lemma proved by Rudra [8] extends Thommesen's result from the binary case to the q-ary case. We show the analogous quantum result – a quantum code from the family of concatenated quantum codes with the outer code being a quantum Generalized Reed-Solomon (QGRS) code [9, 10, 11, 12] and random inner stabilizer codes of rate one almost surely attains the QGVB. We use the family of QGRS codes given by Li, Xing and Wang [11] and give its parameters in Theorem 1.

We outline the structure of our proof. Firstly the classical codes induced by the normalizer of rate one q-ary stabilizer codes are rate one q^2-ary classical block codes $C_{\mathcal{N}^{(i)}}$. Secondly, the distance of classical code induced by the normalizer of our outer code is a classical code $C_{\mathcal{N},(\text{out})}$ that meets the Singleton bound. Thirdly, the classical code induced by the normalizer of our concatenated quantum code $C_{\mathcal{N}}$ is the concatenation of $C_{\mathcal{N},(\text{out})}$ and inner classical codes $C_{\mathcal{N}^{(i)}}$. Then we use Thommesen's technique of finding a lower bound for almost all $C_{\mathcal{N}}$. Using the fact that the distance of nondegenerate quantum codes is equal to the distance of the classical code induced by their normalizers, the quantum result follows from the classical result.

The key difference between Thommesen's proof and ours is that we pick the random inner codes differently from him. Thommesen constructed the generator matrices of the random inner codes by picking each of their entries uniformly at random from the binary alphabet. Such a method when used to construct a set of random n-fold Paulis need not result in a mutually commuting set, and hence may not generate the stabilizer of any quantum stabilizer code. Thus evaluating the probability that a nontrivial Pauli belongs to the normalizer of a uniformly random stabilizer code, which we give as Lemma 4, becomes much more nontrivial than in the analagous classical case. Lemma 4 is the only result from Section 2 that we need to prove the result.

The organization of this paper is as follows: Section 2 defines stabilizer codes from the definition of the Pauli set. Lemma 2 generalizes combinatorial arguments used in Leung and Smith's [13]. We define stabilizer codes using the language of Pauli sets. This leads to an obvious way to pick stabilizer codes uniformly at random. Then we prove Lemma 4. Section 3 introduces our concatenated quantum code construction, and proves that it almost surely attains the QGVB.

2 Group Theory and the Pauli Set

2.1 q-ary Paulis

Let $q \geq 2$ be an integer. Let ω_q be a primitive q-th root of unity, and we choose $\omega_q := e^{2\pi i/q}$. Define $\cdot$ to be the operation for matrix multiplication. '$\cdot$' will be the default binary operation if the binary operation is not specified, and is not to be confused with the inner product of vectors. Define I_q to be the identity operator in $L(\mathbb{C}^q)$.

Now we introduce the ω-commutator, which checks if two elements of $L(\mathbb{C}^q)$ commute up to a phase of ω. The ω-commutator betweem A, B in $L(\mathbb{C}^q)$ is defined as

$$[A, B]_\omega := A \cdot B - (B \cdot A)\omega$$

and is zero if and only if $A \cdot B = (B \cdot A)\omega$.

Now for any binary operator $\square : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$ where $\mathcal{A}$ is a set, define $a^{\square 0}$ to be the identity of $\mathcal{A}$ with respect to $\square$. For all positive integer k, define $a^{\square k} := a \square a^{\square k-1}$. For all $\sigma \in L(\mathbb{C}_q)$, define $\sigma^{\cdot k} := \sigma^k$ for notational simplicity.

Now define q-ary Paulis $X, Z \in L(\mathbb{C}^q)$ where $X^q = Z^q = I_q$, and the following commutation relations hold.

$$[X, Z]_{\omega_q} := X \cdot Z - \omega_q(Z \cdot X) = 0$$

We obmit showing the binary operator for scalar multiplication. Define the **Pauli set** [1] of order n to be $\mathcal{P}_n$ for integer $n \geq 1$ to be a set where

$$\mathcal{P}_1 := \{X^a \cdot Z^b | a, b \in \mathbb{Z}_q\}$$
$$\mathcal{P}_n := \mathcal{P}_1^{\otimes n}.$$

If $\sigma = I_q^{\otimes n}$, $\sigma \in \mathcal{P}_n$ is a **trivial Pauli** , otherwise σ is a **nontrivial Pauli**.

Now define $\star : \mathcal{P}_n \times \mathcal{P}_n \to \mathcal{P}_n$ to be a binary operation that multiplies Pauli matrices modulo the phases. Clearly $(\mathcal{P}_n, \star)$ is a group. For any $G \subseteq \mathcal{P}_n$ or any $G \in (\mathcal{P}_n)^m$ for integer $m \geq 1$, let $\langle G, \star \rangle$ denote the set generated by G with respect to the $\star$ operation. Following Gottesman [4], we introduce introduce an isomorphism $\varphi_G : (\mathcal{P}_n, \star) \to (\mathbb{Z}_q^{2n}, +)$. In particular for all $a_i, b_i \in \mathbb{Z}_q$ for all $i \in [n]$ define

$$\varphi_G(X^{a_1} \otimes ... \otimes X^{a_n} \otimes Z^{b_1} \otimes ... \otimes Z^{b_n}) := (a_1, ..., a_n, b_1, ..., b_n).$$

This isomorphism allows us to define independence of elements in the Pauli set.

Definition 1 (Independence of elements of a subset of $\mathcal{P}_n$) *$\mathcal{A} \subseteq \mathcal{P}_n$ is a set of independent Paulis if $\{\varphi_G(x) : x \in \mathcal{A}\}$ is a linearly independent set of vectors.*

We similarly define the independence of a tuple of Paulis.

Definition 2 (Independence of subsets of $\mathcal{P}_n$) *Let $\mathcal{A}, \mathcal{B} \subseteq \mathcal{P}_n$. If $\langle \mathcal{A}, \star \rangle \cap \langle \mathcal{B}, \star \rangle = I_q^{\otimes n}$, then we say that $\mathcal{A}$ and $\mathcal{B}$ are* **independent**.

For $\mathbf{x}, \mathbf{y} \in (\mathcal{P}_n)^\ell, \ell \geq 1$, if $\langle \mathbf{x}, \star \rangle \cap \langle \mathbf{y}, \star \rangle = I_q^{\otimes n}$, we say $\mathbf{x}$ and $\mathbf{y}$ are **independent**. We similarly define the independence of two tuples of Paulis. Now we phrase Proposition 10.4 of Nielsen and Chuang [14] in our framework.

Lemma 1 *Let $\mathbf{g} = (g_1, ..., g_\ell)$ be any ℓ-tuple of independent elements from $\mathcal{P}_n$, and $\mathbf{b} = (b_1, ..., b_\ell)$ be any element of $\mathbb{Z}_q^\ell$. Then there exists an $\sigma \in \mathcal{P}_n$ such that for all $i \in [\ell]$ $[x, g_i]_{\omega_q^{b_i}} = 0$.*

Proof: Define $\mathbf{y_j} := \varphi_G(g_j) = (y_{j,1}, ..., y_{j,2n})$ for all g_j. By definition of $\mathbf{g}$, the set of vectors $\{\mathbf{y_1}, ..., \mathbf{y}_\ell\}$ is a linearly independent set of vectors over $\mathbb{Z}_q^{2n}$. Thus the system of linear equations

$$\mathbf{x} \cdot \mathbf{y_j} = b_j, \quad j = 1, ..., \ell \tag{2.1}$$

always has some non-zero solution $\mathbf{x} \in (\mathbb{Z}_q^*)^{2n}$. Let $\mathbf{x}$ be a solution to (2.1). Let $\mathbf{y_j}^{(0)} := (y_{j,1}, ..., y_{j,n}), \mathbf{y_j}^{(1)} := (y_{j,n+1}, ..., y_{j,2n})$, and $\mathbf{x}^{(0)} := (x_1, ...x_n), \mathbf{x}^{(1)} := (x_{n+1}, ...x_{2n})$. Then

$$\mathbf{x}^{(1)} \cdot \mathbf{y}_j^{(1)} - (-\mathbf{x}^{(0)}) \cdot \mathbf{y}_j^{(0)} = b_j, \quad j = 1, ..., \ell$$

Define $\sigma := (X^{x_{n+1}} \otimes ... \otimes X^{x_{2n}}) \cdot (Z^{-x_1} \otimes ... \otimes Z^{-x_n}) \in \mathcal{P}_n$. Then

$$[\sigma, g_j]_{(\omega_q)^{b_j}} = (\omega_q)^{\mathbf{x}^{(1)} \cdot \mathbf{y}^{(1)} - (-\mathbf{x}^{(0)}) \cdot \mathbf{y}^{(0)}} g_j \sigma - (\omega_q)^{b_j} g_j \sigma = 0. \quad \blacksquare$$

[1] The Pauli set is the projective Pauli group, that is, the Pauli group modulo the phases.

Lemma 2 *Let $A = (a_1, ..., a_\ell)$ be a tuple of independent elements from $\mathcal{P}_n$. For all $\mathbf{b} = (b_1, ..., b_\ell) \in \mathbb{Z}_q^\ell$ define*

$$\Omega_{A,\mathbf{b}} := \{y \in \mathcal{P}_n : [y, a_i]_{(\omega_q)^{b_i}} = 0 \quad \forall i \in [\ell]\}.$$

Then for all $\mathbf{b} \in \mathbb{Z}_q^\ell$, $\Omega_{A,\mathbf{b}}$ is a coset of $\Omega_{A,\mathbf{0}}$ in $\mathcal{P}_n$. Also there are q^ℓ cosets of $\Omega_{A,\mathbf{0}}$, each corresponding to a particular $\Omega_{A,\mathbf{b}}$, and $|\Omega_{A,\mathbf{b}}| = q^{2n-\ell}$ for all $\mathbf{b} \in \mathbb{Z}_q^\ell$.

Proof: Now $(\Omega_{A,\mathbf{0}}, \star)$ is the image of the centralizer of A with respect to matrix multiplication under the homomorphism φ, and is thus a group. Since $(\Omega_{A,\mathbf{0}}, \star)$ is a subgroup of $(\mathcal{P}_n, \star)$, it partitions $\mathcal{P}_n$ into cosets. By Lemma 1, for every $\mathbf{b} \in \mathbb{Z}_q^\ell$ there exists a $\sigma \in \mathcal{P}_n$ such that $\sigma \star \Omega_{A,\mathbf{0}} = (\Omega_{A,\mathbf{b}}, \star)$. Thus there are $|\mathbb{Z}_q^\ell| = q^\ell$ cosets of $(\Omega_{A,\mathbf{0}}, \star)$ and by the Lagrange's Theorem, $|(\Omega_{A,\mathbf{0}}, \star)| = q^{2n-\ell}$. ■

Another useful isomorphism is $\varphi : (\mathcal{P}_n, \star) \to (GF(q^2), +)$ for q being a prime power [5]. Now we define φ formally. $\forall \sigma_1 \in \mathcal{P}_1$ s.t. $\sigma_1 = X^a \cdot Z^b, a, b \in \mathbb{Z}_q$, $\boxed{\varphi(\sigma_1) := a\beta + b\beta^{pm} \in GF(q^2)}$ $\forall \sigma \in \mathcal{P}_n$ s.t. $\sigma = \sigma_1 \otimes ... \otimes \sigma_n, \sigma_j \in \mathcal{P}_1 \quad \forall j \in [n]$, $\boxed{\varphi(\sigma) := (\varphi(\sigma_1), ..., \varphi(\sigma_n)) \in GF(q^2)^n}$. $\forall \Sigma \subseteq \mathcal{P}_n$, $\boxed{\varphi(\Sigma) := \{\varphi(\sigma) | \sigma \in \Sigma\} \subseteq GF(q^2)^n}$. In fact, we introduce the $\star$ binary operator so that the map φ is an isomorphism from $(\mathcal{P}_n, \star)$ to $(GF(q^2)^n, +)$.

2.2 q-ary Stabilizer Codes

Our definition of stabilizer codes differs from previous definitions [4, 15] by including information on the code's basis. We use the framework of the Pauli set and include information on the code's coset structure. Our definition is necessary to define random stabilizer codes in the framework of the Pauli set.

Firstly we define a stabilizer independently from a stabilizer code. The normalizer of our stabilizer is really its centralizer.

Definition 3 (Stabilizer, Normalizer) *A set $\mathcal{S} \subseteq \mathcal{P}_n$ is a stabilizer of dimension m if $(\mathcal{S}, \star)$ is a group, $x \cdot y = y \cdot x$ for all $x, y \in \mathcal{S}$, and $|\mathcal{S}| = q^m$. The normalizer of S is $\mathcal{N}(\mathcal{S}) := \{x \in \mathcal{P}_n : x \cdot y = y \cdot x \quad \forall y \in \mathcal{S}\}$.*

Lemma 3 *Let $\mathcal{S}$ be a random stabilizer of size q^ℓ, and $\sigma \in \mathcal{P}_n$ be any nontrivial Pauli. Then* $\Pr[\sigma \in \mathcal{N}(\mathcal{S})] \leq q^{-\ell}$.

Proof: If $\ell = 0$ then $\mathcal{N}(\mathcal{S}) = \mathcal{P}_n$ and $\sigma \in \mathcal{P}_n$ by definition. Thus $\Pr[\sigma \in \mathcal{N}(\mathcal{S})] = 1 = q^{-0}$. Now assume $\ell \in [n]$. Let A be the number of ways to pick $g = (g_1, ..., g_\ell)$ such that $\langle g, \star \rangle$ is a stabilizer of size q^ℓ. Then the number of stabilizers of size q^ℓ is $A/\ell!$. We pick g by picking the $g_i's$ sequentially. The number of ways to pick g_1 is the number of non-trivial Paulis which is $(q^{2n} - 1)$. The set of Paulis that commute with $(g_1, ..., g_i)$ is $\Omega_{(g_1,...,g_i),\mathbf{0}}$. Again $\langle (g_1, ..., g_i), \star \rangle \subset \Omega_{(g_1,...,g_i),\mathbf{0}}$. Hence the number of ways to pick g_{i+1} is $|\Omega_{(g_1,...,g_i),\mathbf{0}}| - q^i = q^{2n-i} - q^i$ by Lemma 2. Hence $A = \frac{1}{\ell!} \prod_{i=0}^{\ell-1} (q^{2n-i} - q^i)$.

Let B be the number of ways to pick $h = (h_1, ..., h_\ell)$ such that $\mathcal{S} = \langle h, \star \rangle$ is a stabilizer of size q^ℓ and $\sigma \in \mathcal{N}(\mathcal{S})$. Then the number of stabilizers of size q^ℓ whose normalizer contains σ is $B/\ell!$. We pick h by picking the $h_i's$ sequentially. The set of all Paulis that commutes with σ is $\Omega_{(\sigma),(0)}$. Moreover the identity is in $\Omega_{(\sigma),(0)}$. Thus the number of ways to pick h_1 is

$|\Omega_{(\sigma),(0)}| - 1 = q^{2n-1} - 1$ by Lemma 2. The set of Paulis that commute with $(\sigma, h_1, ..., h_i)$ is $\Omega_{(\sigma,h_1,...h_i),\mathbf{0}}$. Again $\langle (h_1, ..., h_i), \star \rangle \subset \Omega_{(\sigma,h_1,...,h_i),\mathbf{0}}$. Hence the number of ways to pick h_{i+1} is $|\Omega_{(\sigma,h_1,...,h_i),\mathbf{0}}| - q^i = q^{2n-i-1} - q^i$ by Lemma 2. Hence $B = \frac{1}{\ell!}\prod_{i=0}^{\ell-1}(q^{2n-i-1} - q^i)$.

Thus the required probability is $(B/\ell!)/(A/\ell!) = B/A \leq q^{-\ell}$. ■

Corollary 1 *Let $\mathcal{S}$ be a random stabilizer of size q^ℓ, and $\sigma \in \mathcal{P}_n$ be any nontrivial Pauli. Then* $\Pr[\sigma \in \mathcal{N}(\mathcal{S})\backslash\mathcal{S}] \leq q^{-\ell}$.

Definition 4 (Stabilizer code, Heisenberg picture) *Let*

$$(\mathcal{S}, \bar{X}_1 \star \mathcal{S}, ..., \bar{X}_k \star \mathcal{S}, \bar{Z}_1 \star \mathcal{S}, ..., \bar{Z}_k \star \mathcal{S})$$

be a $[[n,k]]_q$ stabilizer code in the Heisenberg picture, where $\mathcal{S} \subseteq \mathcal{P}_n$ is a stabilizer of size q^{n-k}, and $\bar{X}_1, ..., \bar{X}_k, \bar{Z}_1, ..., \bar{Z}_k \in \mathcal{N}(\mathcal{S})$ such that for all $i, j \in [k]$, $[\bar{X}_i, \bar{Z}_j]_{(\omega_q)^{\delta_{ij}}} = 0$.

Definition 5 (Cosets of a Stabilizer Code) *Let a $[[n,k]]_q$ code in the Heisenberg picture be $C = (\mathcal{S}, \bar{X}_1 \star \mathcal{S}, ..., \bar{X}_k \star \mathcal{S}, \bar{Z}_q \star \mathcal{S}, ..., \bar{Z}_k \star \mathcal{S})$. Let $\mathbf{c} = (x_1, ..., x_k, z_1, ..., z_k) \in \mathbb{Z}_q^{2k}$ label the cosets of $\mathcal{S}$. Then the cosets of C are defined as*

$$\mathcal{S}_{\mathbf{c}} := \left(\bar{X_1}^{\star x_1} \star ... \star \bar{X_k}^{\star x_k}\right) \star \left(\bar{Z_1}^{\star z_1} \star ... \star \bar{Z_k}^{\star z_k}\right) \star \mathcal{S}.$$

$\mathcal{S}_{\mathbf{0}}$ is the **trivial coset** *of C. All other cosets of C are* **nontrivial cosets** *of C.*

From the previous definition it follows that

$$(\mathcal{S}, \bar{X}_1 \star \mathcal{S}, ..., \bar{X}_k \star \mathcal{S}, \bar{Z}_1 \star \mathcal{S}, ..., \bar{Z}_k \star \mathcal{S}) = (\mathcal{S}_{\mathbf{0}}, \mathcal{S}_{\mathbf{e_1}}, ..., \mathcal{S}_{\mathbf{e_{2k}}})$$

where $\mathbf{e_i}$ are the natural basis vectors for $\mathbb{Z}_q^{2k}$ for all $i \in [2k]$. For given stabilizer code $C = (\mathcal{S}_{\mathbf{0}}, \mathcal{S}_{\mathbf{e_1}}, ..., \mathcal{S}_{\mathbf{e_{2k}}})$, define $\psi_C(\phi\mathcal{S}_{\mathbf{c}}) := \varphi_G^{-1}(\mathbf{c})$. Then the map $\psi_C : \{\mathcal{S}_{\mathbf{c}} : \mathbf{c} \in \mathbb{Z}_q^{2k}\} \to \mathcal{P}_k$ is an isomorphism with respect to matrix multiplication. Let us also define $\psi_C : \mathcal{P}_n \to \mathcal{P}_k$ such that $\psi_C(a) = \psi_C(\mathcal{S}_{\mathbf{c}})$ for all $a \in \mathcal{S}_{\mathbf{c}}$.

Definition 6 (Random Stabilizer Code) *Let $\mathfrak{S}$ be the set of all stabilizers of size q^{n-k}. Pick $\mathcal{S} \in \mathfrak{S}$ uniformly at random. Let $\mathfrak{C}_{\mathcal{S}}$ be the set of all stabilizer codes with stabilizer $\mathcal{S} \in \mathfrak{S}$. Pick $C \in \mathfrak{C}_{\mathcal{S}}$ uniformly at random. Then C is a random $[[n,k]]_q$ stabilizer code.*

Lemma 4 *Given any nontrivial Pauli $\sigma \in \mathcal{P}_n$, nonzero $\mathbf{c} \in \mathbb{Z}_q^{2k}$, and a random $[[n,k]]_q$ stabilizer code $C = (\mathcal{S}_{\mathbf{0}}, \mathcal{S}_{\mathbf{e_1}}, ..., \mathcal{S}_{\mathbf{e_{2k}}})$, the probability that $\sigma \in \mathcal{S}_{\mathbf{c}}$ is no greater than $q^{-(n+k)}$.*

Proof: First we evaluate the probability that $\sigma \in \mathcal{S}_{\mathbf{c}}$ given that σ belongs to a nontrivial coset of $\mathcal{S}$. We use the fact that the set of cosets of $\mathcal{S}$ are isomorphic to $\mathcal{P}_k$ under the map ψ.

Let A be the number of all stabilizer codes with stabilizer $\mathcal{S}$. Let $x = (x_1, ..., x_k), z = (z_1, ..., z_k) \in \mathcal{P}_k^k$ be tuples that generate stabilizers of size q^k. We also want $[x_i, z_j]_{(\omega_q)^{\delta_{ij}}} = 0$. By the proof of Lemma 3, the number of ways to pick z is $\prod_{i=0}^{k-1}(q^{2n-i} - q^i)$. We pick x by picking the $x_i's$ sequentially. We pick x_1 from the set $\Omega_{(z_1,...,z_k),\mathbf{e_1}}$, $\mathbf{e_1}$ is the standard basis vector of appropriate length. Similarly, for $i \geq 2$ we pick x_i from the set $\Omega_{(z_1,...,z_k,x_1,...x_{i-1}),\mathbf{e_i}}$. By the commutation properties that the x_i's must obey, they must be mutually independent and independent of all the z_i's. Thus the ways to pick x given z is $(q^{2k-k})(q^{2k-k-1})...(q) = q^{k(k+1)/2}$ by Lemma 2 . Hence $A = q^{k(k+1)/2}\prod_{i=0}^{k-1}(q^{2n-i} - q^i)$.

Let $\mathbf{c} = (a_1, ..., a_k, b_1, ..., b_k)$. Let B be the number of all stabilizer codes with σ in $\mathcal{S}_\mathbf{c}$. Let $x' = (x'_1, ..., x'_k), z' = (z'_1, ..., z'_k) \in \mathcal{P}_k^k$ be tuples that generate stabilizers of size q^k, such that $\psi_C(\sigma) = \psi_C(\mathcal{S}_\mathbf{c}) = \star_{i=1}^k ({x'}_i^{\star a_i} \star {z'}_i^{\star b_i})$. Let $\bar{\sigma} = \psi_C(\sigma)$. We also want $[x'_i, z'_j]_{(\omega_q)^{\delta_{ij}}} = 0$. Since $\mathbf{c} \neq \mathbf{0}$, we have only two cases: (1) $a_\alpha \neq 0$ for some $\alpha \in [k]$; (2) $b_\beta \neq 0$ for some $\beta \in [k]$. Let $\pi = (\alpha\ k)$ be a permutation.

When case (1) holds, $\bar{\sigma}$ is independent of the tuple z'. Thus we pick z' first. Now $z'_1 \in \Omega_{(\bar{\sigma}),(a_1)}$. Hence the number of ways to pick z'_1 is $|\Omega_{(\bar{\sigma}),(a_1)} \backslash I^{\otimes n}| = q^{2n-1} - 1$ by Lemma 2. For $i \in [k-1]$, is $z'_{i+1} \in \Omega_{(\bar{\sigma}, z'_1, ..., z'_i),(a_i, 0, ..., 0)}$. Since $\langle (z'_1, ..., z'_i), \star \rangle \subset \Omega_{(\bar{\sigma}, z'_1, ..., z'_i),(a_i, 0, ..., 0)}$, the number of ways to pick z'_{i+1} given $(z'_1, ..., z'_i)$ is $|\Omega_{(\bar{\sigma}, z'_1, ..., z'_i),(a_i, 0, ..., 0)}| - q^i = q^{2n-i-1} - q^i$ by Lemma 2. Hence the number of ways to pick z' is $\prod_{i=0}^{k-1}(q^{2n-i-1} - q^i)$. We pick x' by picking the ${x'}'_i s$ in the order ${x'}_{\pi(1)}, ..., {x'}_{\pi(k-1)}$. Let $\mathbf{e'_i}$ be a standard basis vector of length k. Then, $x'_{\pi(1)} \in \Omega_{(\bar{\sigma}, z'_1, ..., z'_k),(-b_\pi(i), \mathbf{e}_{\pi(\mathbf{1})})}$ and $x'_{\pi(i+1)} \in \Omega_{(\bar{\sigma}, z'_1, ..., z'_k, x'_\pi(1), ..., x'_{\pi(i)}),(-b_\pi(i+1), \mathbf{e'}_{\pi(\mathbf{i})}, 0, ..., 0)}$ for all $i \in [k-1]$. Each of the $x'_{\pi(i+1)}$ are independent of the preceding $x'_{\pi(i)}$'s and $\bar{\sigma}$ for $i \in [k-2]$ by definition of π. Hence the number of ways to pick x' given z' is $(q^{2k-k-1})(q^{2k-k-2})...(q) = q^{k(k-1)/2}$. A similar argument holds for case (2), with the roles of x' and z' reversed. Hence $B = q^{k(k-1)/2} \prod_{i=0}^{k-1}(q^{2n-i-1} - q^i)$.

Thus the probability $\sigma \in \mathcal{S}_\mathbf{c}$ given that $\sigma \in \mathcal{N}(\mathcal{S}) \backslash \mathcal{S}$ is $B/A \leq q^{-2k}$. By Corollary 1, the probability that σ belongs to a nontrivial coset of $\mathcal{S}$ is no greater than $q^{-(n-k)}$. Thus the probability that $\sigma \in \mathcal{S}_\mathbf{c}$ is no greater than $q^{-2k} q^{-(n-k)} = q^{-(n+k)}$. ■

3 The Main Result

Concatenated codes are created by two levels of encoding. The "outer code" refers to the first level of encoding. The "inner codes" refer to the second level of encoding. The $N = q^n$ inner codes are $[[n, n]]_q$ independently chosen random stabilizer codes. q is a fixed prime power.

A classical code with parameters $[N, K, D]_q$ is MDS if $D = N - K + 1$. A quantum code with parameters $[[N, K, D]]_q$ is MDS if $D = (N - K)/2 + 1$ [2] We use the following quantum outer code.

Theorem 1 (Li, Xing, Wang [11]) *Let N be a prime power. Then for all integer K in $[0, N]$ such that $N - K$ is even, there exist $[[N, K, D]]_N$ quantum MDS codes. Their normalizers are classical MDS codes under φ, with known generator matrices.*

The following theorem is the main result. Its proof follows Thommesen's proof [7] closely, except for Lemma 5.

Theorem 2 *Construct a $[[nN, nNR, d]]_q$ quantum code by concatenating $N = q^n$ random $[[n, n]]_q$ inner quantum codes with an $[[N, NR]]_N$ outer quantum code given by Theorem 1. Then for all $R \in [0, 1]$ such that $NR - q$ is even, $n \geq 2$, with probability at least $1 - q^{n-(1-R)q^n \bar{f}(q)}$,*

$$\frac{d}{nN} \geq H_{q^2}^{-1}\left(\frac{1-R}{2}\right) - \frac{4\bar{f}(q)}{n(1-R)}$$

where $\bar{f}(q) := \dfrac{\log_q 2}{\log_{q^2}\left[(q^2-1)\left(\frac{2}{H_{q^2}^{-1}(1/2)} - 1\right)\right]}$.

[2] If a quantum stabilizer MDS code is nondegenerate, its normalizer under the map φ is a classical MDS code.

Let the normalizer of the outer quantum code be $\mathcal{N}^{(\mathrm{out})}$ and the normalizers of the inner quantum codes be $\mathcal{N}^{(i)}$. Let the normalizer of our concatenated code be $\mathcal{N}$. Let $C_{\mathcal{N},(\mathrm{out})} := \varphi(\mathcal{N}^{(\mathrm{out})}), C_{\mathcal{N}^{(i)}} = \varphi(\mathcal{N}^{(i)}), C_{\mathcal{N}} = \varphi(\mathcal{N})$ be the corresponding classical codes. $C_{\mathcal{N},(\mathrm{out})}$ is a classical MDS code by Theorem [11] and has distance D. Thus the number of its codewords of weight w is [16]

$$A_w \leq \binom{N}{w}(q^{2n})^{w-D+1}, \quad D \leq w \leq N. \tag{3.1}$$

As our inner codes have a rate of 1, $C_{\mathcal{N}}$ is the concatenation of $C_{\mathcal{N},(\mathrm{out})}$ with the inner codes $C_{\mathcal{N}^{(i)}}$. Thus there is a bijection from each codeword of $\tilde{u}$ of $C_{\mathcal{N}}$ to each codeword u of $C_{\mathcal{N},(\mathrm{out})}$. Let C_w denote the set of codewords in $C_{\mathcal{N},(\mathrm{out})}$ with Hamming weight w.

Lemma 5 *Let $u = (u_1, ..., u_N) \in C_w$, $N \geq w \geq D$. Then for all $y \in GF(q^2)^{nN}$,*

$$\Pr[y = \tilde{u}] \leq q^{-2nw}.$$

Proof: Let $y \in GF(q^2)^{nN}$, $y = (y_1, ..., y_N)$ and $y_j \in GF(q^2)^n$ for all $j \in [N]$. Let $T := \{\tilde{u} : u \in C_w\}$. If $y \notin T$, then $\Pr[y = \tilde{u}] = 0$. For all $y \in T$, y is a nonzero q^2-ary vector of length nN on exactly w blocks. Let y_i be any nonzero q^2-ary vector of length n on one block. Let nonzero $\mathbf{c} = \varphi_G(\varphi^{-1}(u_i)) \in \mathbb{Z}_q^{2n}$ label the stabilizer coset $\mathcal{S}_{\mathbf{c}}$ that u_i corresponds to. Then $\Pr[y_i = \tilde{u}_i] = \Pr[\varphi^{-1}(y_i) \in S_{\mathbf{c}}] = q^{-2n}$ by Lemma 4. Each inner code is chosen independently, so the result follows. ■

Lemma 6 *$\forall u \in C_w$, $N \geq w \geq D$, and $\frac{h}{nw} \leq \frac{q^2-1}{q^2}$,$\Pr[\mathrm{wt}(\tilde{u}) \leq h] \leq (q^2)^{nwH_{q^2}(\frac{h}{nw})-nw}$*

Proof:

$$\Pr[\mathrm{wt}(\tilde{u}) \leq h] \leq \sum_{\mathrm{wt}(y)\leq h} \Pr[y = \tilde{u}] \leq \left(\sum_{j=0}^{h} \binom{nw}{j}(q^2-1)^j\right) q^{-2nw}$$

The first inequality is from the union bound. The next inequality comes from Lemma 5 and knowing the size of the q^2-ary Hamming ball of radius h. Since $\frac{h}{nw} \leq \frac{q^2-1}{q^2}$, we upper bound the size of q^2-ary Hamming balls [16] to get $\Pr[\mathrm{wt}(\tilde{u}) \leq h] \leq (q^2)^{nwH_{q^2}(\frac{h}{nw})}(q^2)^{-nw}$. ■

3.1 Proof of Theorem 2

The theorem is vacuous for $R = 1$ so assume $0 \leq R < 1$ without loss of generality. Let R_N be the rate of $C_{N,(\mathrm{out})}$. Now $d \geq \mathrm{mindist}(C_N)$ (see Appendix), so we obtain a lower bound on the distance of mindist(C_N).

$$\begin{aligned}
\Pr[d \le h] &\le \sum_{\mathbf{0}\neq u\in\mathcal{C}_{N,(\mathrm{out})}} \Pr\left[\mathrm{wt}(\tilde{u}) \le h\right] && \text{, union bound}\\
&= \sum_{w=D}^{N} \binom{N}{w} (q^{2n})^{w-D+1} \Pr\left[\mathrm{wt}(\tilde{u}) \le h\right] && \text{, (3.1)}\\
&\le \sum_{w=D}^{N} 2^N (q^{2n})^{w-D+1} \Pr\left[\mathrm{wt}(\tilde{u}) \le h\right] && , \binom{N}{w} \le 2^N\\
&\le \sum_{w=D}^{N} 2^N (q^{2n})^{w-D+1} (q^2)^{nwH_{q^2}(\frac{h}{nw})-nw} && \text{, Lemma 6}\\
&= \sum_{w=D}^{N} (q^2)^{-nw\delta} < Nq^{-nN(1-R)\delta} && , \frac{w}{N} \ge 1-R_N = \frac{1-R}{2}\\
&= q^{n-nq^n(1-R)\delta} && , N = q^n
\end{aligned}$$

where $\epsilon = \frac{N\log_q 2}{nw}$ and

$$\delta = -\left((1-\frac{D}{w}+\frac{1}{w}) + H_{q^2}(\frac{h}{nw}) - 1 + \epsilon\right). \tag{3.2}$$

Since $H_{q^2}^{-1}$ is an increasing function, by rearranging (3.2) we get the following.

$$\begin{aligned}
\frac{h}{nw} &= H_{q^2}^{-1}\left(-\epsilon - (1-\frac{D}{w}+\frac{1}{w}) + 1\right) - \delta\\
\frac{h}{nN} &= \frac{w}{N}H_{q^2}^{-1}\left(-\epsilon-\theta+1\right) - \frac{w}{N}\delta && \text{, Set } \theta := 1-\tfrac{D}{w}+\tfrac{1}{w}\\
&< \frac{w}{N}H_{q^2}^{-1}\left(1-\theta\right) - \frac{w}{N}\epsilon\left(\frac{1}{\log_{q^2}\left[(q^2-1)\left(\frac{2}{H_{q^2}^{-1}(1-\theta-\epsilon)}-1\right)\right]}+\delta\right) && \text{, Lemma 7}
\end{aligned}$$

Since $\frac{w}{N} = \frac{1-R_N}{1-\theta}$ and $0 \le \theta \le R_N$,

$$\begin{aligned}
\frac{h}{nN} < &\min_{0\le\theta\le R_N} \frac{1-R_N}{1-\theta} H_{q^2}^{-1}\left(1-\theta\right)\\
&- \max_{0\le\theta\le R_N} \frac{1-R_N}{1-\theta}\epsilon\left(\frac{1}{\log_{q^2}\left[(q^2-1)\left(\frac{2}{H_{q^2}^{-1}(1-\theta-\epsilon)}-1\right)\right]}+\delta\right)
\end{aligned} \tag{3.3}$$

From Rudra's refinement of Thommesen's result (Lemma 8),

$$\min_{0\le\theta\le R_N} \frac{1-R_N}{1-\theta} H_{q^2}^{-1}\left(1-\theta\right) = H_{q^2}^{-1}\left(1-R_N\right) = H_{q^2}^{-1}\left(\frac{1-R}{2}\right). \tag{3.4}$$

Moreover $\frac{\log_q 2}{n} \le \epsilon = \frac{N\log_q 2}{nw} < \frac{2\log_q 2}{n(1-R)}$ because $1 \ge \frac{w}{N} \ge \frac{1-R}{2}$. Thus for $n \ge 2\log_q 2$

$$\frac{h}{nN} < H_{q^2}^{-1}\left(\frac{1-R}{2}\right) - (\epsilon f(q) + \delta)$$

where $f(q) := \left(\log_{q^2}\left[(q^2-1)\left(\frac{2}{H_{q^2}^{-1}(1/2)}-1\right)\right]\right)^{-1}$. It suffices to pick $n \geq 2$. Now pick $\delta = \epsilon f(q)$. Then

$$\frac{h}{nN} < H_{q^2}^{-1}\left(\frac{1-R}{2}\right) - 2\epsilon f(q).$$

Thus with probability at least $1 - q^{n-nN(1-R)\frac{\log_q 2}{n}f(q)} = 1 - q^{n-N(1-R)(\log_q 2)f(q)}$, the concatenated code has relative distance at least $H_{q^2}^{-1}(\frac{1-R}{2}) - \frac{4\log_q 2}{n(1-R)}f(q)$. ■

4 Acknowledgements

The author wishes to thank Debbie Leung and William Matthews for many helpful comments. The author also wishes to thank the Lazaradis Fellowship for financial support.

5 Appendix

5.1 q-ary Entropy and Related Functions

Let $q \geq 4$ be an integer and $H_q(x) := x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x)$ be the q-ary entropy function. The q-ary entropy function is increasing for $x \in [0, 1-1/q)$ so we can define $H_q^{-1} : [0,1] \to [0, 1-1/q]$ to be the inverse function of $H_q : [0, 1-1/q] \to [0,1]$. Observe then that H_q^{-1} is also an increasing function on the domain where it is defined.

Lemma 7 *For all $q \geq 2$, for all $y \in (0, 1-1/q)$, and for all $\epsilon \in (0, y)$, we have*

$$H_q^{-1}(y-\epsilon) \leq H_q^{-1}(y) - \epsilon(\log_q[(q-1)(\frac{2}{H_q^{-1}(y-\epsilon)}-1])^{-1}.$$

Proof: Let f be the restriction of H_q such that $f : (0, 1-1/q) \to (0,1)$. Now f is continuous and bijective on the open interval. Let $b = f(a)$. By the inverse function theorem, $(f^{-1})'(b) = (f'(a))^{-1}$ for all $b \in (0,1)$. Now for all $b \in (0,1)$, $f'(b) = \log_q(q-1) + \log_q(1-b) - \log_q(b)$ and so f is concave. Thus $(f^{-1})'(b) = (\log_q[(q-1)(1/a-1)])^{-1}$ and f^{-1} is convex. Thus $f^{-1}(y-\epsilon) \leq f^{-1}(y) - \epsilon(f^{-1})'(y-\epsilon) = f^{-1}(y) - \epsilon(\log_q[(q-1)(\frac{2}{f^{-1}(y-\epsilon)}-1)]^{-1}$. ■

Lemma 8 (Rudra) *Let $q \geq 2$ be an integer. For any $0 \leq y \leq 1$,*

$$\min_{0\leq\theta\leq y} \frac{1}{1-\theta}H_q^{-1}(1-\theta) = \frac{1}{1-y}H_q^{-1}(1-y).$$

5.2 Stabilizer codes and classical codes

Let us have a $[[n,k,d]]_p$ stabilizer code with stabilizer $\mathcal{S}$ and normalizer $\mathcal{N}$. Define $C_{\mathcal{S}} := \varphi(\mathcal{S})$ and $C_{\mathcal{N}} := \varphi(\mathcal{N})$. By definition $C_{\mathcal{S}} \subset C_{\mathcal{N}}$. The distance d of our stabilizer code is define as

$$d := \min\{\mathrm{wt}(x) | x \in C_{\mathcal{N}} \backslash C_{\mathcal{S}}\}$$

Since $C_{\mathcal{S}}, C_{\mathcal{N}} \subset GF(p^2)^n$, we can identify them as p^2-ary block codes of block length n. Denote a classical block code by $(n', M', d')_p$ if it a set of M' strings of length n over an alphabet of size p, and with minimum distance d'. Then $C_{\mathcal{S}} = (n, p^{n-k}, d_S)_{p^2}$ and $C_{\mathcal{N}} = (n, p^{n+k}, d_N)_{p^2}$. $C_{\mathcal{N}} \backslash C_{\mathcal{S}} \subset C_{\mathcal{N}} \implies d \geq d_N$. If $d = d_N$ we say our stabilizer code is nondegenerate, and if $d > d_N$ we say that our stabilizer code is degenerate.

References

[1] A. Ashikhmin, S. Litsyn, and M. A. Tsfasman, "Asymptotically good quantum codes," *Phys. Rev. A*, vol. 63, no. 3, p. 032311, 2001.

[2] H. C. amd San Ling and C. Xing, "Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound," *IEEE Transactions on Information Theory*, vol. 47, pp. 2055–2058, July 2001.

[3] R. Matsumoto, "Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes," *IEEE Transactions on Information Theory*, vol. 48, pp. 2122–2124, July 2002.

[4] D. Gottesman, *Stabilizer Codes and Quantum Error Correction.* PhD thesis, California Institute of Technology, 1997. quant-ph/9705052.

[5] A. Ashikhmin and E. Knill, "Nonbinary stabilizer codes," *IEEE Transactions on Information theory*, vol. 47, pp. 3065–3072, Nov 2001. quant-ph/0005008v1.

[6] Y. Ma, "The asymptotic probability distribution of the relative distance of additive quantum codes," *Journal of Mathematical Analysis and Applications*, vol. 340, pp. 550–557, 2008.

[7] C. Thommesen, "The existence of binary linear concatenated codes with Reed-Solomon outer codes which asymptotically meet the Gilbert-Varshamov bound," *IEEE transactions on information theory*, vol. 29, no. 6, pp. 850–853, 1983.

[8] A. Rudra, *List Decoding and Property Testing of Error Correcting Codes.* PhD thesis, University of Washington, 2007.

[9] M. Grassl, W. Geiselmann, and T. Beth, "Quantum Reed-Solomon codes," *Proceedings Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-13), Springer Lecture Notes in Computer Science*, p. 1719, 1999.

[10] M. Grassl, T. Beth, and M. Roetteler, "On optimal quantum codes," *International Journal of Quantum Information*, vol. 2, no. 1, pp. 55–64, 2004.

[11] Z. Li, L. Xing, and X. Wang, "Quantum generalized Reed-Solomon codes: Unified framework for quantum maximum-distance-separable codes," *Phys. Rev. A*, vol. 77, no. 1, p. 012308, 2008.

[12] Z. Li, L.-J. Xing, and X.-M. Wang, "A family of asymptotically good quantum codes based on code concatenation," *CoRR*, vol. abs/0901.0042, 2009.

[13] D. Leung and G. Smith, "Communicating over adversarial quantum channels using quantum list codes," *IEEE transactions on information theory*, vol. 54, no. 2, pp. 883–887, 2008.

[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, second ed., 2000.

[15] P. Sarvepalli, *Quantum Stabilizer Codes and Beyond.* PhD thesis, Texas A & M University, 2008. quant-ph/arXiv:0810.2574.

[16] F. J. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes.* north-holland publishing company, first ed., 1977.